REMARKS

Claims 1-45 remain pending in the Application. Claims 1-45 stand rejected by the Examiner. Applicant traverses the rejections of claims 1-45.

Claim Rejections

Claims 1-10, 16-25, and 31-40 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Vanstone et al. U.S. Patent No. 5,761,305 (hereinafter the "Vanstone reference"). The office action also used the following reference: Alfred Menezes et al. *Handbook of Applied Cryptography* (hereinafter the "Applied Cryptography reference"). Claims 11-15, 26-30, and 41-45 stand rejected as being unpatentable over the Vanstone and the Applied Cryptography references and further in view of Boyd et al.'s "Key Establishment Protocols for Secure Mobile Communications." Applicant traverses these rejections.

Claim 1 recites that a plaintext message is encrypted into a ciphertext message and in the encrypting step, an ephemeral key pair is produced. That ephemeral key pair is then used in signing a digital signature. The Examiner maintains that the Vanstone reference discloses the limitations of claim 1. Applicant respectfully disagrees.

Cryptography usually involves two distinct stages: key establishment and encryption/decryption. The Vanstone reference acknowledges the two distinct stages:

> Key establishment is the process by which two (or more) parties establish a shared secret key, called the session key. The session key is subsequently used to achieve some cryptographic goal, such as privacy. (Vanstone , col. 1, ll. 29-32).

In other words, in the first stage, called key establishment, two or more parties (in this context, computer systems) exchange information to establish a shared key, called a session key. Then, once the session key is established, it is subsequently used in the second stage (e.g., called

encryption/decryption). In the encryption/decryption stage, the sending party converts a message from what is known as "plaintext" to "ciphertext" by applying a mathematical transformation, which may be reversed only with the session key.

The two stages are independent. In some cryptographic approaches, the first stage may not even involve an automatic key establishment, and thus, keys may be exchanged manually, for example over the phone, and then manually entered in the computer systems. Furthermore, once keys have been exchanged, by any method, the information does not have to be encrypted. Also, some information may be encrypted and some may not.

In general, the Vanstone reference is directed to the first stage in that the Vanstone reference discloses a method of overcoming deficiencies of previously known key establishment methods. The title of the Vanstone reference shows the sharp focus on the first stage: "Key agreement and transport protocol with implicit signatures." The Vanstone reference discloses stage 1 methods of exchanging the keys for providing better security (e.g., the Vanstone reference "...provide[s] a method of establishing a session key between a pair of correspondents A, B to permit exchange of information therebetween, ..." (col. 2, ll. 62-64)). This "exchange of information" is not part of the first stage methods mentioned in the Vanstone reference. Rather the methods disclosed in the Vanstone reference are performed to enable a later secure exchange of information. Although the Vanstone reference may disclose methods using digital signatures, Vanstone is only using the digital signatures as a part of a stage 1 key establishment process. Accordingly, the Vanstone reference does not disclose the use of digital signatures in the encryption stage (e.g., when plaintext is encrypted).

More specifically, claim 1 of the present application recites a public key encryption process and system comprising the steps of: (a) encrypting a plaintext message into a cyphertext message, the encrypting step includes the step of producing an ephemeral key pair; (b) signing a digital

signature using the ephemeral key pair. The method of claim 1 is directed to a stage 2 (e.g., later stage) encryption process. At this second stage, the plaintext message is being encrypted, and consequently, element (b), signing a digital signature, is a part of the encryption method.

The examiner cites Vanstone at col. 3, lines 1-7 and lines 39-43 for disclosing the limitations of step (a) of claim 1. Vanstone at col. 3, lines 1-7 is as follows:

> i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power g(x) to provide a first exponentiated function $f(\alpha)^{g(x)}$;
> ii) said first correspondent A generating a first signature s_A from said random integer x and said first exponentiated function $f(\alpha)^{g(x)}$; ...

Applicant respectfully disagrees that this passage of Vanstone discloses the limitations of step (a) of claim 1. For example, steps (i) and (ii) of Vanstone are not used to encrypt a plaintext message into a ciphertext message as required by claim 1. Instead the paragraph prior to this passage in Vanstone states that these steps (i) and (ii) are used in "a method of establishing a session key between a pair of correspondents A, B to permit exchange of information therebetween" (col. 2, ll. 62-64). "The session key is then used to achieve some cryptographic goal, such as privacy" (see col. 1, ll. 29-32). The established session key of Vanstone is not part of the encryption step as required in step (a) of claim 1 and therefore this passage in Vanstone does not disclose the limitations of step (a) of claim 1.

Moreover, the instances in Vanstone of using a digital signature cited by Examiner (i.e., Vanstone, col. 3, ll. 1-10; col. 4, ll. 62-64) disclose using digital signatures in the stage 1 key establishment process. This is evident because the cited sections are not referring to digital signatures in the context of encrypting a plaintext message (which is a later stage operation) as required by claim 1.

Also with reference to claim 1, the Examiner maintains on page 3 of the office action that

"although the phrase 'ephemeral key pair' does not appear in the Vanstone reference, Vanstone's key pair is generated each time it is needed, without repetition and discarded once used, which by definition makes it an ephemeral key pair." Applicant respectfully disagrees. Vanstone states that the public key (which with the private key forms the key pair) is "issued by a trusted center" (see Vanstone, col. 4, l. 1). Accordingly, the key pairs in Vanstone are not ephemeral as required by claim 1.

For such reasons, claim 1 as well as all claims dependent thereon, are patentable over the Vanstone reference. The other independent claims (e.g., claims 16 and 31), in combination with their respective limitations, are directed to stage 2 processing and thus are allowable over the cited references. Because each of the pending independent claims are allowable, their respective dependent claims are also allowable.

Applicant also disagrees with other positions presented by the Examiner. For example, Applicant disagrees with the position of the Examiner with respect to claim 4. Claim 4 recites:

> 4. (ORIGINAL) A public-key encryption process according to claim 1, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key $X = xG$, where G is a generator.

The Examiner maintains that Vanstone discloses the limitations of claim 4 at col. 3, lines 1-5 and that the Applied Cryptography reference at section 8.4 and Algorithm 8.17 does so as well. However, these passages are directed to key generation for use in a stage 1 key establishment process and do not disclose generating an encryption ephemeral private key and calculating an encryption ephemeral public key as required by claim 4. Accordingly, claim 4 is allowable for this additional reason.

CONCLUSION

For the foregoing reasons, Applicant respectfully submits that claims 1-45 are allowable. Therefore, the Examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

Date: June 7, 2005

By: _____

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939